US008990950B2

(12) United States Patent
Kruger et al.

(10) Patent No.: US 8,990,950 B2
(45) Date of Patent: Mar. 24, 2015

(54) ENABLING GRANULAR DISCRETIONARY ACCESS CONTROL FOR DATA STORED IN A CLOUD COMPUTING ENVIRONMENT

(75) Inventors: **Stephen P. Kruger**, Malahide (IE); **Olgierd S. Pieczul**, Clonsilla (IE)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 782 days.

(21) Appl. No.: **12/979,117**

(22) Filed: **Dec. 27, 2010**

(65) **Prior Publication Data**

US 2012/0167197 A1 Jun. 28, 2012

(51) **Int. Cl.**

G06F 17/30	(2006.01)
G06F 12/00	(2006.01)
G06F 21/31	(2013.01)
G06F 21/10	(2013.01)
G06F 21/62	(2013.01)

(52) **U.S. Cl.**

CPC ***G06F 17/30*** (2013.01); ***G06F 12/00*** (2013.01); *G06F 21/31* (2013.01); *G06F 21/10* (2013.01); *G06F 21/62* (2013.01)

USPC **726/26**; 726/27; 726/28; 726/29; 726/30; 707/781

(58) **Field of Classification Search**

CPC G06F 17/30; G06F 21/31; G06F 21/10; G06F 21/62; G06F 12/00

USPC 726/26–30; 707/781, E17.005

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2003/0126465	A1	7/2003	Tassone et al.	
2003/0188198	A1*	10/2003	Holdsworth et al.	713/201
2007/0214144	A1*	9/2007	Lawson et al.	707/9
2008/0082538	A1*	4/2008	Meijer et al.	707/9
2009/0228950	A1	9/2009	Reed et al.	
2009/0228967	A1	9/2009	Ghadegesin et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

CN	20101523365 A	9/2009

OTHER PUBLICATIONS

Yu, Ting, et al., "Security Policy Testing via Automated Program Code Generation (Extended Abstract)," CSIIRW, Apr. 13-15, 2009.

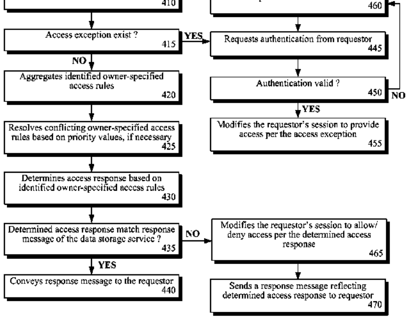
(Continued)

Primary Examiner — Kaveh Abrishamkar
Assistant Examiner — Ayoub Alata
(74) *Attorney, Agent, or Firm* — Patents on Demand P.A.; Brian K. Buchheit; Scott M. Garrett

(57) ABSTRACT

Enabling discretionary data access control in a cloud computing environment can begin with the obtainment of a data request and response message by an access manager service. The response message can be generated by a data storage service in response to the data request. The access manager service can identify owner-specified access rules and/or access exceptions applicable to the data request. An access response can be determined using the applicable owner-specified access rules and/or access exceptions. Both the response message and the access response can indicate the allowance or denial of access to the requested data artifact. The access response can be compared to the response message. If the access response does not match the response message, the response message can be overridden to express the access response. If the access response matches the response message, the response message can be conveyed to the originating entity of the data request.

18 Claims, 5 Drawing Sheets


400
Obtains data request and response message determined by the data storage service 405
Identifies applicable owner-specified access rules and/or exceptions for data request 410
Access exception exist ? 415
YES
NO
Aggregates identified owner-specified access rules 420
Resolves conflicting owner-specified access rules based on priority values, if necessary 425
Determines access response based on identified owner-specified access rules 430
Determined access response match response message of the data storage service ? 435
NO
YES
Conveys response message to the requestor 440
Informs requestor of invalid authentication 460
Requests authentication from requestor 445
Authentication valid ? 450
NO
YES
Modifies the requestor's session to provide access per the access exception 455
Modifies the requestor's session to allow/ deny access per the determined access response 465
Sends a response message reflecting determined access response to requestor 470